FIGURE 2 is a flow chart illustrating a method for secure data transmission in accordance with an embodiment of the present invention; and

FIGURE 3 is a flow chart illustrating a method for secure data transmission in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

The preferred embodiments of the present invention and the advantages thereof are best understood by referring to FIGURES 1 through 3 of the drawings, like numerals being used for like and corresponding parts of the various drawings.

FIGURE 1 is a diagram illustrating a system 10 for secure data transmission in accordance with an embodiment of the present invention. In the illustrated embodiment, information or data is communicated via the Internet 12 between a sender 14 and a recipient 16. For example, in the illustrated embodiment, the sender 14 and recipient 16 comprise a client 18 communicating with a server 20, respectively, via the Internet 12; however, it should be understood that other communication components and other communication mediums, such as, but not limited to, local area networks or wide area networks, may also be used. Additionally, as will be further described below, the present invention may be used for secure data transmission from the client 18 to the server 20 or from the server 20 to the client 18.

In the illustrated embodiment, the client 18 comprises a processor 30 coupled to a memory 32. The present invention also encompasses computer software that may be stored in the memory 32 and executed by the processor 30. In this embodiment, the client 18 comprises a string generator 40, a hashing engine 42, an encryption engine 44, and a signature generator 46, which are computer software programs. In FIGURE 1, the string generator 40, hashing engine 42, encryption engine 44, and signature generator 46 are illustrated as being stored in the memory 32, where they can be executed by the processor 30. Briefly, the string generator 40, hashing engine 42, and encryption engine 44 are used to encrypt the data to be transmitted to the server 20 by the client 18. The signature generator 46 generates a signature for

transmitting from the client 18 to the server 20 for authenticating the data transmission and the identity of the client 18.

The client 18 illustrated in FIGURE 1 also comprises a database 50. In the illustrated embodiment, the database 50 comprises key data 52, character string data 53, signature data 56, and transmission data 58. The key data 52 comprises information associated with keys used to identify the client 18 and to encrypt and decrypt the data transmitted from the client to the server 20. For example, in the illustrated embodiment, the key data 52 comprises an identification key 60 used to identify the client 18. For example, the identification key 60 may comprise a serial number or other type of identifier indicating the particular client 18 transmitting the data. The key data 52 also comprises a private key 62 and a hash key 64. Briefly, the hash key 64 is generated using the private key 62. The hash key 64 is then used to encrypt and decrypt the transmitted data.

In the illustrated embodiment, the transmission data 58 comprises unencrypted data 70 and encrypted data 72. The data 70 comprises information provided by a user of the client 18 intended to be transmitted to the server 20 in an unencrypted or decrypted format. The encrypted data 72 comprises an encrypted format of the data 70 which is transmitted to the server 20 via the Internet 12.

In operation, the string generator 40 randomly generates and stores the character string 54 in the database 50. The hashing engine 42 hashes the character string 54 with the private key 62 to generate the hash key 64, which is also stored in the database 50. The encryption engine 44 then encrypts the data 70 using the hash key 64 as an encryption password. As briefly described above, the encrypted data 72 may also be stored in the database 50. The processor 30 then transmits the character string 54, the encrypted data 72, and the identification key 60 to the server 20 via the Internet 12. Decryption of the encrypted data 72 by the server 20 will be described in greater detail below. Additionally, although identified as an "encryption" engine 44, it should be understood that the encryption engine 44 may be used to either encrypt or decrypt data; however, the present invention may also be configured using separate encrypting and decrypting components.

The signature generator 46 generates and stores the signature 56 in the database 50 by hashing the hash key 64 with the data 70. The processor 30 also

transmits the signature 56 to the server 20 via the Internet 12. Authentication or verification of the transmitted data and the identity of the client 18 by the server 20 using the signature 56 will be described in greater detail below.

In the illustrated embodiment, the server 20 also comprises a processor 80 coupled to a memory 82. The present invention also encompasses computer software that may be stored in the memory 82 and executed by the processor 80. In this embodiment, the server 20 comprises a string generator 84, a hashing engine 86, a decryption engine 88, and a signature engine 90, which are computer software programs. In FIGURE 1, the string generator 84, hashing engine 86, decryption engine 88, and signature engine 90 are illustrated as being stored in the memory 82, where they can be executed by the processor 80. Briefly, the hashing engine 86, decryption engine 88, and signature engine 90 are used to decrypt and verify or authenticate the data received from the client 18. The string generator 84 is used for generating a random character string in connection with transmitting data from the server 20 to the client 18 in a similar manner as described above. Additionally, although identified as a "decryption" engine 88, it should be understood that the decryption engine 88 may be used to either encrypt or decrypt data.

The server 20 also comprises a database 100 accessible by the processor 80. In the illustrated embodiment, the database 100 comprises relational data 102 and transmission data 104. The relational data 102 comprises information associated with relating encryption and decryption keys for each of the clients 18 to the transmitted identification keys 60. For example, in the illustrated embodiment, the relational data 102 comprises identification keys 108 and private keys 110 arranged in a look-up table or other format such that for each identification key 108, a matching or corresponding private key 110 may be identified. Accordingly, the identification keys 60 and 108 and the private keys 62 and 110 are correlated so that data encryption and decryption may be performed at each end of the data transmission path.

The transmission data 104 comprises information associated with the data received from the client 18. For example, in the illustrated embodiment, the transmission data 104 comprises encrypted data 112 and decrypted data 114. The encrypted data 112 comprises the information received from the client 18 via the Internet 12 in an encrypted format. Accordingly, the decrypted data 114 comprises